AMENDMENTS TO THE SPECIFICATION

Please amend paragraph [00018] as follows:

Embodiments of the invention may be implemented in one or a combination of hardware, firmware, and software. Embodiments of the invention may also be implemented as instructions stored on a machine- accessible medium, which may be read and executed by a computing platform to perform the operations described herein. A machine-accessible medium may include any mechanism for storing or transmitting information in a form readable by a machine (e.g., a computer). For example, a machine- accessible medium may include read only memory (ROM); random access memory (RAM); magnetic disk storage media; optical storage media; flash memory devices; ~~electrical, optical, acoustical or other form of propagated signals (e.g., carrier waves, infrared signals, digital signals, etc.)~~, and others.

Please amend paragraph [00020] as follows:

To implement this bare-metal configuration and attestation, the target client computer, for example, a consumer desktop or a rack-server in a data-center, may have a Trusted Platform Module (TPM). The TPM may be described by the specifications ~~found at~~available from the Trusted Computing Group (TCG), an Oregon nonprofit corporation ~~website, http://www.trustedcomputinggroup.org~~. In addition to having the TPM on the target client computer, the firmware of the target client computer may also have firmware that performs a hash-extend operation of any installed code and data into a respective platform configuration register (PCR). The hash-extend operation may be a one-way hash operation performed by the TPM using a TPM_EXTEND command.

Please amend paragraph [00040] as follows:

The terms "computer program medium" and "computer usable medium" are used here to refer generally to media such as, but not limited to, removable storage drive 614, and a hard disk

installed in hard disk drive 612~~, and signals 628~~. These computer program media are means for providing software to computer system 600.